Osterman Research

WHITE PAPER

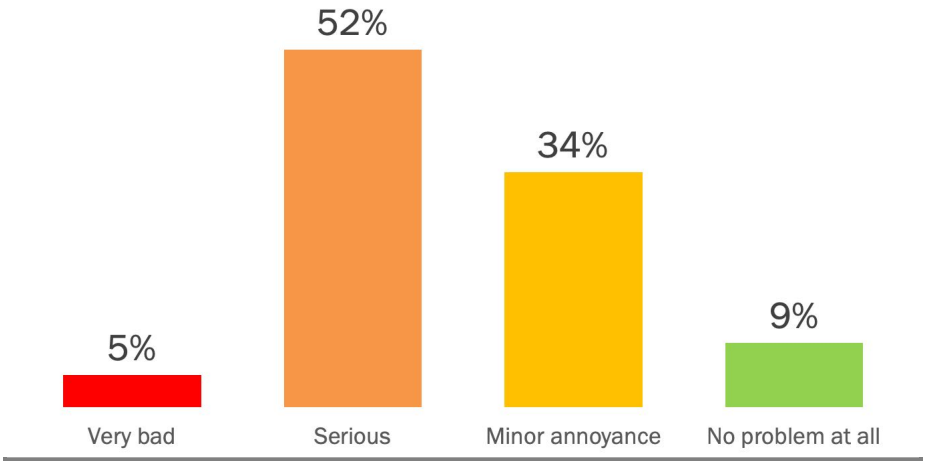
White Paper by Osterman Research
Published **October 2020**
Sponsored by **Anomali**

How to Minimize the Impact of the Cybersecurity Skills Shortage

Executive Summary

In the face of a relentless increase in the number and sophistication of cyber-attacks, organizations need to strengthen their security defenses, improve their overall readiness to ward off new and emerging attacks, and have the ability to recover (and learn) from attacks and incidents that get through current protections. Cybersecurity professionals are essential to the defense of organizations, but the bad news is that skilled professionals are in short supply. As shown in Figure 1, nearly three out of five of the cybersecurity professionals we surveyed for this white paper consider the shortage to be either "serious" or "very bad".

Figure 1
Cybersecurity Professionals' Views on the Cybersecurity Skills Shortage



Source: Osterman Research, Inc.

Organizations across the world have unfilled cybersecurity vacancies, and the cybersecurity professionals already on staff are pushed to their limits. Something must change to address the staff shortages that are limiting organizations' ability to erect and maintain strong defenses. In this paper, we examine the cybersecurity skills shortage and advocate the use of advanced security services and technologies that more effectively leverage the time of current professionals.

The strategy of hiring increasing numbers of cybersecurity professionals with the right skill set is dead.

KEY TAKEAWAYS

- Protecting an organization from the many varieties of cyber threats is a challenging mandate, and it is trending toward greater complexity. The market supply of cybersecurity professionals is far less than the market demand, and the role itself is difficult, complex and frequently overwhelming.

- The strategy of hiring increasing numbers of cybersecurity professionals with the right skill set is dead. The rising volume and variety of cyber threats, plus the global supply shortage, means a different strategy is needed that revisits the balance between people, process and technology in cybersecurity is needed.

- Advanced security services and technology providers that offer automation capabilities, leverage artificial intelligence and machine learning, and provide orchestration and aggregation of multiple, disparate security solutions offer high potential for addressing the cybersecurity skills shortage.

- While the cybersecurity skills shortage is a visceral experience for organizations, addressing the shortage through advanced services and technology providers raises several implications that must be taken account of in a thoughtful way,

such as facilitating the entry of the next generation of cybersecurity professionals into the market, and shortening the learning curve of new technologies.

ABOUT THIS WHITE PAPER AND SURVEY

This white paper was sponsored by Anomali; information about the company is provided at the end of the paper. This paper references data from an in-depth survey of 130 cybersecurity professionals in mid-sized and large organizations that was conducted specifically for this paper – the complete set of data from that survey will be published shortly after publication of this paper.

Scoping the Skills Shortage

Protecting an organization from the many varieties of cyber threats is a challenging mandate—for organizational leadership, technology vendors, and the cybersecurity professionals on the front lines of defense. And it is trending toward greater complexity. In this section, we take a brief look at trends affecting cybersecurity, the market supply data on cybersecurity professionals, the current nature of the cybersecurity professional's role, and the difficulty of hiring cybersecurity professionals.

CURRENT TRENDS

Anyone looking for a dynamic and ever-changing job role, with almost guaranteed employment for life, need look no further than the domain of cybersecurity. While cybersecurity has been a growing issue for quite some time, we've entered a new "perfect storm" of cyber piracy. Consider that:

While cybersecurity has been a growing issue for quite some time, we've entered a new "perfect storm" of cyber piracy.

- The race to embrace the cloud has outpaced the willingness and resources made available to explore and mitigate the security implications of the move, independent of the continent. About half of the companies in the UK who have moved to cloud services have not updated their security strategies,[i] and there is an acute shortage of cybersecurity professionals with competency in cloud security for public, private and hybrid cloud infrastructures.[ii]

- The global health pandemic of 2020 forced many people to suddenly work from home, and the shift from well-protected corporate office environments to ad hoc, remote and untested locations intensified the security challenges for organizations and the pressures on cybersecurity professionals. COVID-19 themed phishing emails came thick and fast, unpatched home routers provided new entry points for attackers, and personal, unmanaged devices were used for corporate work. The City of New York faced almost a 10x increase in the number of endpoints it had to secure and manage when employees moved home.

- Being a hacker or cybercriminal is a more attractive alternative to many young people than being a cybersecurity professional or defender. Almost half of under-25-year-olds would prefer to use hacking skills for fun, secretive activities or financial gain, instead of fighting against the same.[iii] That is, the supply of hackers and other cybercriminals is not going down.

- The potential attack surface is growing. Beyond the explosion in remote work, the Internet of Things (IoT), the emergence of smart buildings and connected cities, the adoption of self-driving vehicles, and the merging of IT infrastructures with operational technology at power plants, water treatment locations and transportation networks creates new threat vectors that we don't sufficiently protect yet, let alone adequately understand.

- Cybercriminals are not standing still, they also keep innovating with new technologies and business methods, applying artificial intelligence and machine learning to create ever-changing threats to reduce the likelihood of detection, and evolving the "as-a-service" criminal ecosystem. It's not surprising that more

than 90 percent of cybersecurity professionals believe cybercriminals outgun them, and that their organizations are vulnerable to a significant cyber-attack.[iv]

MARKET SUPPLY OF CYBERSECURITY PROFESSIONALS

There have been many estimates of supply shortages for cybersecurity professionals in recent years, along with several forecasts looking multiple years into the future. Consider this chronology of the evolving problem in the United States:

- In 2014, the U.S. Bureau of Labor Statistics forecast the number of security jobs to increase 18 percent over the coming decade.
- In 2015, Peninsula Press said over 200,000 cybersecurity jobs in the United States were currently available, and that there had been a 74 percent increase in job postings since 2010.
- In 2016, the Harvey Nash and KPMG CIO Survey concluded that CIOs were being hindered by "the greatest skills shortage since the Great Recession" of 2007, and said that demand for security skills jumped by 17 percent year-over-year.
- In 2017, the Center for Cyber Safety and Education Global Information Security Workforce Study found that over two thirds of information security professionals said their organization was understaffed for information security.
- In 2019, the U.S. Bureau of Labor Statistics said the job outlook for information security analysts was expected to grow by 31 percent over the coming decade, a significant lift from its 2014 forecast. Cyber Seek calculated there were over 300,000 unfilled cybersecurity roles in the United States, and only 2.3 current workers compared to job openings, less than half the national average of 5.8 for all job types.
- In 2020, Cyber Seek said the number of job openings had increased to just under 510,000, and the ratio of current workers to job openings had dropped to only 1.8.

The news isn't any better on the global stage, with common estimates in recent years of global supply shortages ranging from 1.5 million to three million or more.

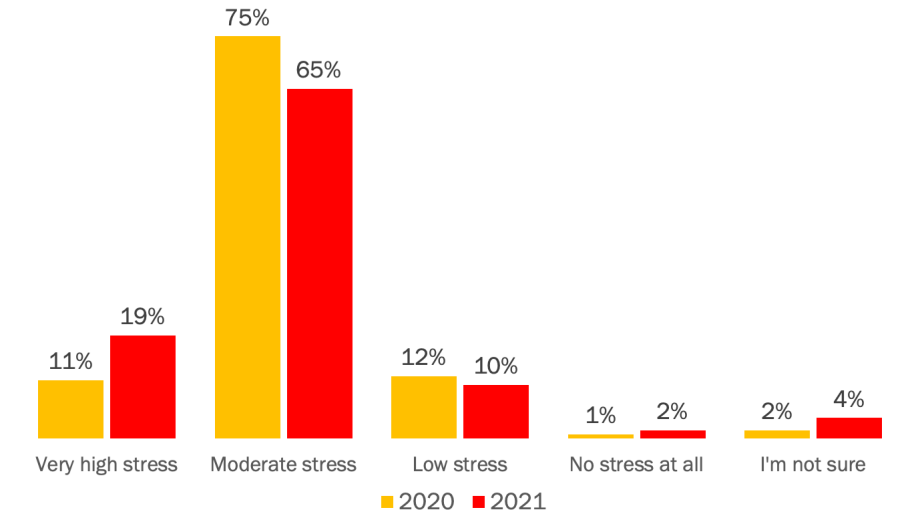
The role of the cybersecurity professional is difficult, complex and frequently overwhelming.

ASSESSING THE ROLE OF THE CYBERSECURITY PROFESSIONAL

The role of the cybersecurity professional is difficult, complex and frequently overwhelming:

- Information overload, increased workloads, and elevated stress due to new data protection regulations and other current trends are commonly felt by professionals. A highly demanding workload goes with the territory, due to the use of multiple, non-integrated security systems, not enough cybersecurity professionals on the team, and the growing attack surface. The survey conducted for this white paper found that one in nine cybersecurity professionals is experiencing "very high stress" levels and this is expected to increase to nearly one in five in just a year's time, as shown in Figure 2.

Figure 2
Current and Anticipated Stress Level for Security Team Staff Members
2020 and 2021



Source: Osterman Research, Inc.

- Hackers, attackers and cybercriminals have access to sophisticated cyber weaponry, including as-a-service threat offerings to streamline new malicious campaigns. Over two fifths of respondents to a Cisco study say they have basically settled into a response-only mode, cleaning up after an attack but no longer attempting proactive defense.

- It's a job that's almost doomed to failure, and repeated failure at that. "Assume you've been breached" is common advice across the cybersecurity industry, which doesn't engender feelings of efficacy in cybersecurity professionals for their ability to do a great job. More than 90 percent of cybersecurity professionals believe cybercriminals outgun them, and that their organizations are vulnerable to a significant cyber-attack.[v]

- Even CIOs have low confidence that their organization can identify and respond to cyber-attacks, although confidence levels have risen slightly for the first time in five years.[vi]

- The frantic pace of the work means cybersecurity professionals are not investing enough time in ongoing skill development and training programs. If continued for too long, security professionals fall even further behind in the cyber arms race, and cyber protections for organizations are undermined.

Even CIOs have low confidence that their organization can identify and respond to cyber-attacks.

DIFFICULTIES IN HIRING FOR CYBERSECURITY ROLES

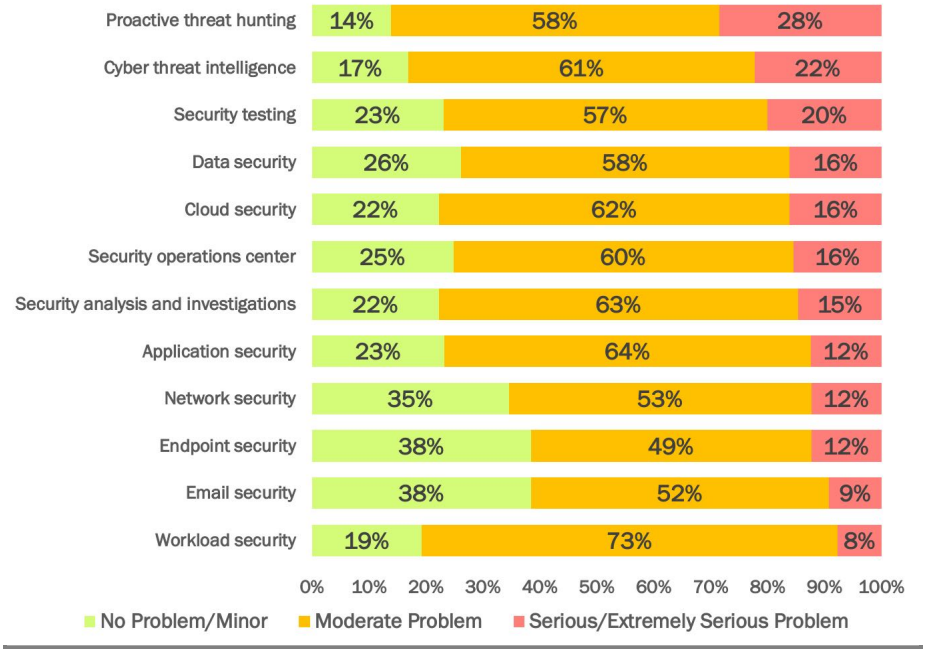
As an implication of the generalized dearth of market supply for cybersecurity roles, organizations experience a significant time lag in filling available positions. This plays out in several ways:

- Fewer people apply for cybersecurity job roles than apply for all other types of job roles in corporate environments. Two-thirds of organizations receive fewer than five applications for new cybersecurity roles, compared with 60 to 250 for other corporate roles.[vii]

- Filling cybersecurity roles can take more than six months—if they are filled at all. As the seniority and years of experience required for the job role increases, so does the duration of the hiring timeframe.[viii] The result is that key roles within

security go unfilled or severely understaffed, creating major problems for organizations' cybersecurity posture, as shown in Figure 3.

Figure 3
Degree to Which Current Security Staffing and Skill Levels are a Problem



Source: Osterman Research, Inc.

- Cybersecurity professionals are actively headhunted for new roles with offers of higher salaries, bonuses and improved working conditions. Employers have to counter-offer with elevated incentives to retain current employees, or face losing security professionals with a good understanding of how the business operates, and then having to seek out new talent in a supply-challenged market.

- As the threat landscape becomes more complex and ever-changing with the greater embrace of cloud and mobile technologies, new hires often lack the depth of experience and training to hit the ground running. Organizations have to complement high salaries with ongoing investment in training and certification.

- Filling some job roles is just really difficult, because of the emergence of new complex multi-domain threats. For example, using advanced technology to create smart buildings, self-driving vehicles, and smart cities elevates the consequences of a successful attack, where a phishing email that results in lost credentials can result in a weaponized building that threatens human life. People with the security competence to address these new and emerging threats are few and far between.

- Finding the right mix of skills in a given cybersecurity professional is challenging. While many excel in technical competencies, few also have the communication skills needed for effectively engaging with the wider organization about security defenses, practices and processes.

New hires often lack the depth of experience and training to hit the ground running.

Addressing the Skills Gap – A New Strategy

A conventional strategy of hiring increasing numbers of cybersecurity professionals with the right skill set is impractical, if not impossible. The rising volume and variety of cyber threats, plus the global supply shortage, means a different strategy is needed. The three-pronged approach of people, process and technology has to be re-balanced in light of the marketplace realities:

- Skilled people are essential, but the supply shortage means organizations will have to better leverage the time and energy of the cybersecurity professionals they do have on-staff, reduce as much as possible manual processes that are ripe for automation, and commit to better ongoing skill development for current and new staff.

- Effective processes are essential, but this is only partly about breach identification, incident response and threat detection. The more fundamental security processes that can close off avenues of attack need to be designed and implemented across the organization, and this requires cybersecurity professionals with both strategic security design skills and available time.

- Improved services and technology are essential, both to better leverage the time and energy of cybersecurity professionals, and also to reduce by design the attack surface and attack vectors available for cybercriminals.

- Third-party vendors and outsourced services are also a key element in solving the skills shortage because they can be used to offload many of the tasks and services that in-house staff cannot do or would be strained to do in a complete and timely manner.

Third-party vendors and outsourced services are also a key element in solving the skills shortage.

ON TRAINING

Better ongoing skill development for current and new staff is part of the answer for addressing the shortage of cybersecurity skills. Better training means:

- Skills of current staff members are kept up-to-date in order to address new and evolving security threats.

- Current staff members cultivate mastery in the new advanced security applications and platforms introduced to the organization, enabling a more effective match between what the technology can offer and how it is put to use. While many advanced security technologies are available, they rely on skilled personnel to put them to best use.

- Staff members are more likely to stay with an organization when they experience the investment in their ongoing training, which has long-run benefits for the organization in retaining skilled staff with a good understanding of the landscape of the organization in addition to security principles and practices. A new cybersecurity professional may bring the latter with them, but the former takes time to develop.

- New hires move from inexperienced to making a contribution much faster, hence speeding the time-to-value for new cybersecurity professionals.

- Greater likelihood of developing strong and resilient security practices across the organization, taking into consideration the current threat landscape. Broader and deeper skill competencies give cybersecurity professionals the ability to see beyond the latest flurry of alerts to the more fundamental changes needed for proactive defense.

ON TECHNOLOGY

Several types of advanced security technologies offer the prospect of leveraging the time and energy of cybersecurity professionals. These technologies complement and enhance – rather than replace entirely – the work of such professionals, and include such ideas as speeding up specific processes, automating tasks through predefined workflows, and using artificial intelligence methods to crunch through ever-large datasets to identify and prioritize threats.

The economics works like this: if a current set of tasks requires five full-time equivalent (FTE) cybersecurity professionals, then advanced technologies that streamline certain tasks, automate others, and in general reduces some of the manual effort required only has to deliver a 20 percent leverage per person to enable the same five to do the work of six FTEs. Since many organizations are already struggling to fill "the sixth role" due to the acute global supply shortage, advanced technology offers the potential of eliminating the need to do so. Any technology that can reliably create a time leverage across the tasks done by cybersecurity professionals can contribute to reducing the impact of the cybersecurity skills shortage. For example:

- Resetting passwords as a manual process can take three to five minutes per request. Self-service automation eliminates this task almost entirely, with security staff only having to deal with the few exceptional cases each week.

- Collating data from multiple, disparate security solutions incurs time cost in the form of app switching, working with different interfaces, and manually creating synthesized profiles of threats. This time cost has been estimated at 20 percent of a security analyst's working day, which could be removed entirely through automatic correlation.

- Managing access rights as employees move across job roles and departments is a process that has to be done with speed and precision in order to reduce the likelihood of inadvertent access to sensitive data by unauthorized personnel or malicious actors who have compromised a user's account. As a manual process, it's ripe for error and delay, and takes time to get right every time. As an automated process with self-service request and approval workflows, along with policy-based access updates, both the time and potential for inadvertent error is removed.

- Sorting through hundreds or thousands of daily security alerts to decide where to start is an impossible task to carry out without automated analysis. Even merely reading the description of each alert will consume several hours each day, let alone deciding which of the many are the few to deal with first. Advanced security tools that can group alerts for individual threat events, enrich alerts with contextual data related to the threat landscape of the organization and wider threat intelligence services, and highlight the priority issues largely eliminate the read-and-decide mental cycles and time incurred by security professionals. Additionally, such tools can be ever watchful for new alerts and threats to dynamically change the ranking of priority events.

- Addressing the low value, high volume repetitive tasks through automation, process streamlining and managed security services gives cybersecurity professionals the ability to focus on higher value tasks that require strategic planning, space to think, and latitude to play with different ideas. A security professional who no longer has to deal with an unending stream of warnings, requests and alerts can turn their attention to the more fundamental aspects of securing the organization, protecting its data, and improving compliance with new data protection regulations.

Several types of advanced security technologies offer the prospect of leveraging the time and energy of cybersecurity professionals.

Solutions and Services to Consider

In this section we look at four advanced security solutions that offer technology capabilities to leverage and complement the skills of cybersecurity professionals. The solutions profiled in this section replace manual efforts with automated ones and embrace advanced technologies for improving security posture.

Advanced security technologies that offer automation capabilities replace time-consuming manual processes with policy-based workflows and playbooks that are executed without human intervention – and with or without human oversight, as required by the organization. A task analysis study of the common tasks undertaken by cybersecurity professionals in your organization will highlight possibilities for replacing high quantities of time spent on manual processes with automated alternatives. Three areas that are ripe for greater automation are identity and access management, malware detection, and vulnerability analysis and patching.

IDENTITY AND ACCESS MANAGEMENT

Automating many of the tasks associated with identity and access management (IAM) eliminates the time spent on these tasks by cybersecurity professionals, and ensures both faster turnaround time and higher levels of adherence to access policies. Automations to develop for IAM include self-service password resets, policy-based workflows for onboarding new employees, self-service requests for access to new applications, and policy-based workflows for revoking access to particular applications when an employee shifts departments, as well as to the entire suite of applications and services when their employment ends. Managerial approvals, application-owner access reviews, and escalations can be created to ensure human oversight and accountability becomes a normal part of day-to-day business operations. Each automation removes 3-30 minutes of manual processing time, and almost perfect adherence to access policies greatly shrinks the threat space if credentials are compromised, since each credential can only gain access to current systems rather than legacy systems for which access hasn't yet been removed. Automated IAM, in other words, can also reduce future time expenditure by cybersecurity professionals since the attacks were eliminated by design.

MALWARE DETECTION

Signature-based approaches for detecting malware are from a bygone era. The use of new technologies by cyber criminals for automatically morphing malware variants so that signatures are nearly unique means that a different approach is required. Behavioral analysis of what a given file does or attempts to execute on an endpoint offers a way of detecting suspicious and malicious payloads, and automation capabilities can be used to automatically remove similar payloads from other repositories, automatically quarantine suspicious files, and even quarantine a potentially-infected endpoint for further analysis by a cybersecurity professional if automated mitigations and roll-back capabilities are ineffective.

VULNERABILITY ANALYSIS AND PATCHING

Automated correlation of threat intelligence updates and newly identified software and application vulnerabilities against a real-time asset register of servers, endpoints and devices enables faster identification and prioritization of vulnerabilities that need to be patched (or that could be patched virtually through an application firewall, for example). While automated patching of 100 percent of vulnerabilities in near-real-time is not yet a reality, a very high proportion of vulnerabilities across servers, endpoints and devices can be automated. Advanced security systems that can automatically patch over 70 percent of identified vulnerabilities shrinks the time required by cybersecurity professionals for hands-on, manual patching by two-thirds or more, and enables security staff to focus on the more challenging patches, e.g., those that require extra validation before going live. One study in 2020 noted that 80 percent of the attacks they observed in the first half of 2020 exploited vulnerabilities that were at least 3 years old, and 20 percent exploited vulnerabilities that were at least seven years old.[ix] Using automated vulnerability analysis and patching helps

Advanced security technologies that offer automation capabilities replace time-consuming manual processes.

keep your organization from falling victim to these older vulnerabilities that should have been patched years ago.

ARTIFICIAL INTLELLIGENCE (AI) AND MACHINE LEARNING (ML)

Advanced security tools that leverage artificial intelligence and machine learning algorithms complement human intellect with automated analysis, reducing the time and effort required by cybersecurity professionals to complete the same analysis—and given that computer systems can track and correlate many more variables than a person, the same analysis by a professional would be nearly impossible. Unlike a specific security product or service, such as a web application firewall or a cloud access security broker from a given vendor, you don't go out and buy an "artificial intelligence" security product or a "machine learning" one. AI and ML capabilities are being integrated into all types of security products, and it is this inclusion that offers hope for the cybersecurity skills shortage. As more advanced AI capabilities get added into current and next generation security products, the time required by security professionals to carry out their job tasks decreases, thus offering a multiplier of current staff.

Examples of AI and ML being included in security products and services include:

- Analysis of patterns of access to cloud services and business applications by employees, taking into consideration variables such as time of day, network location, geographical location, most recent log in (including the geographical location of that access request), and the types of devices used (e.g., whether they are corporately managed or not). Out-of-the-ordinary access patterns can be flagged as suspicious, and either blocked outright or subjected to additional authentication demands or more limited access rights being granted. Such automated and ongoing analysis can enable prompt identification of stolen credentials after a phishing attack (e.g., via the time difference between two log in attempts from geographical locations that are too far apart to enable the individual to physically travel from one to the other in the elapsed time between the two requests), restrict access to sensitive material from unknown devices or never-been-seen-before networks even though the access credentials are valid, and warn or block when an employee suddenly attempts to download thousands of files during the middle of the night from outside an office location.

- Identification of new malware variants, ransomware families and phishing campaigns that have been generated using AI and ML by cybercriminals. With millions of new ML-mutated threats being released daily, the war against this ML-generated scourge cannot function without ML-powered protections.

- Correlation of individual threat signals from different security products in order to cut down thousands of individual signals to tens or hundreds of grouping of related signals. ML algorithms can prioritize the more important threat groupings, so that cybersecurity professionals can focus their time and effort on what matters most, rather than getting caught up in chasing down hundreds of false positives or committing time to threats with very low threat quotients.

- Automated and ongoing comparative analysis of new threat intelligence against historical log and threat signal data, in order to identify earlier breaches or security incidents that passed unnoticed at the time.

- Automated identification of where a given user has greater access rights than they require for their job role, despite being in a role where other equivalent employees do need access. Streamlining access rights reduces a user's privileges to interact with sensitive data, and if they don't need it for their job role, revoke access until they do.

As more advanced AI capabilities get added into current and next generation security products, the time required by security professionals to carry out their job tasks decreases.

- AI and ML capabilities, along with automation tooling, can be set to automatically implement recommendations, mitigate threats, or remediate incidents. Of equal validity, however, is where recommendations require approval and thus facilitate human oversight of the evolving security protections across the organization.

SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE (SOAR)

SOAR platforms are built on the idea that multiple, disparate security solutions may work adequately in isolation, but they work much better together. The three highlight capabilities in SOAR combine, integrate and commonize signals and data from separate security platforms to enable:

- Orchestration, in the sense of pulling together and aggregating the alerts, warnings and threat signals from individual security solutions into an integrated interface with common tooling. Alerts and signals are complemented with the threat intelligence available to the organization, to inform the automatic calculation of relative priority levels. Some SOAR platforms can also account for the relative importance of different applications, data repositories and systems—for example, those that hold sensitive customer data or intellectual property—in calculating a business risk score that is also used in the calculation of priority.

- Automation, in the sense of being able to automatically respond to various incidents and incident types with predefined workflows (which are often called "playbooks"). Stage-gate approvals can be built into automated playbooks if required, so that security professionals can keep an eye on what's happening and what's being recommended. Every alert or incident that is handled automatically is one that a security professional doesn't have to engage with.

- Incident response capabilities, so that when automated playbooks are insufficient and human intervention is required, security professionals are offered an informed snapshot of the incident, all relevant and related data, and the tools required to further analyze the incident and mitigate its effects.

The interaction of these three capabilities means alerts and incidents that can be handled automatically are dealt with quickly and without human intervention, enabling security professionals to focus on the more challenging alerts and incidents for which the initial legwork has already been done. At minimum, SOAR platforms have been shown to double the productivity of security professionals.

THREAT INTELLIGENCE PLATFORM (TIP)

The growing interest in cyber threat intelligence at organizations results from the recognition that it is impossible to stop technically advanced adversaries without foreknowledge of their intentions and methods. Cyber threat intelligence is knowledge about adversaries and their motivations, intentions, and methods. Threat intelligence can be captured from many different sources, including open-source threat feeds, intelligence shared among different community members (e.g. ISACs), commercial threat feeds, and internally discovered threat intelligence. As the security practice at organizations gains more maturity, they usually find themselves seeking to leverage more and different kinds of threat intelligence, but struggle with heavily manual workflows to manage the large amounts of data this entails. This results in limited visibility and slowed detection.

The growing interest in cyber threat intelligence at organizations results from the recognition that it is impossible to stop technically advanced adversaries without foreknowledge of their intentions and methods.

The purpose of a Threat Intelligence Platform is to automate and scale the collection, analysis, and dissemination of threat intelligence. Delivering the right threat intelligence both to security and business staff, as well as directly to security controls in machine readable format, enables better protection of the critical assets of the enterprise. Threat intelligence platforms have several key functions:

- **Data Aggregation**
  A Threat Intelligence Platform automatically collects and reconciles data from

various sources and formats. Ingesting information from a variety of sources is a critical component to a strong security infrastructure.

- **Normalization and Enrichment of Data**
  Collecting data across a wide variety of feeds results in millions of indicators to sort through per day, making it vital to process data efficiently. Processing includes several steps, but is comprised of three main elements -- normalization, de-duplication, and enrichment of data.

- **Security system integration**
  Data that has been normalized, vetted, and enriched can then be delivered to security controls on an automated basis to use for blocking, enforcement and monitoring. Possible security control integrations include SIEM, SOAR, endpoint, firewall, IPS and other systems.

- **Investigation**
  In addition to automatically delivering machine readable threat intelligence, the Threat Intelligence Platform can provide a highly effective platform for threat research and investigation, significantly reducing response time. Some of the common capabilities of TIPs include tools that support threat indicator pivoting and expansion, data enrichment to provide additional context to threats, analytic tools such as integrated sandboxing, analyst workflow processes, and the ability to author and publish finished intelligence that needs to be shared more broadly.

MANAGED SECURITY SERVICES

Managed security services of various types are a key element in addressing the skills shortage because they enable the offloading of many tasks that otherwise would have to be managed by in-house staff members. By shifting some of the burden to managed services, much of the volume of malicious content can be detected, identified and remediated before it ever enters the customer network, thereby freeing in-house staff to deal with the more complex cases that would otherwise not be properly addressed because of lack of time and labor resources.

Implications for Organizations

While the cybersecurity skills shortage is a visceral experience for organizations, addressing the shortage through advanced security services and technologies raises several implications that must be taken account of in a thoughtful way. In this section, we look at two implications.

Addressing the shortage through advanced security services and technologies raises several implications that must be taken account.

ENTRY-LEVEL JOBS FOR NEW CYBERSECURITY PROFESSIONALS

Tracking alerts, collating evidence on incidents, reviewing threat intelligence, and deploying patches are all good, entry-level tasks for a new cybersecurity professional to begin with. These offer on-the-ground experience, showcase the types of threats and incidents that are common to the organization (thus cultivating an awareness of the organization's security context and environment), and enable cybersecurity professionals with greater seniority to monitor and coach new employees. Automating these tasks or transforming their scope significantly through AI and machine learning removes these tasks as options for new professionals. From one point of view, this elimination makes it more difficult for new professionals to start into a cybersecurity role, since a higher level of knowledge is required to be effective with more advanced security tools and processes. The alternate point of view, however, is that the removal of these manual, tedious tasks plus the availability of more advanced security tools enables new professionals to make a larger and better contribution faster. If the tasks won't ever have to be done manually again due to enhanced processes and new technology, then there is no need to know the specific ins-and-outs of legacy manual processes.

EMBRACING THE LEARNING CURVE – AND COPING WITH UNFULFILLED EXPECTATIONS

The new advanced security technologies we have profiled in this report have a learning curve for cybersecurity professionals and organizations alike. The former need to understand how to best utilize the capabilities on offer, which is developed through training, ongoing experimentation, and exposure to the results and anomalies. It also benefits from wider non-technical but related skills, such as data science and how machine learning, for example, can best be used in security. The latter—organizations—face a learning curve of how best to embed the technical capabilities within processes and procedures so that they work for the different groups within the organization.

Finally, there's also a learning curve in the sense that current AI and ML security technologies will appear primitive in comparison to what's available in three to five years, and by starting today, while many benefits will accrue immediately, so will the sense of unfulfilled expectations. Starting the journey sooner rather than later enables early benefits to be captured, but within the context of continually looking at how the technology can develop over the next several years to further enable advanced security defenses. Security vendors are investing heavily in AI and ML cybersecurity technologies to improve their offerings.

Conclusions and Next Actions

The worldwide shortage of people with cybersecurity skills is not going to be solved overnight. While increasing market supply is necessary – both by training new entrants to the job market and cross-training current employees with cybersecurity skills – more people alone will not suffice. Cyber threats are too many and varied for more people alone to be the answer. What's needed, in combination with better training, is the adoption of new advanced security services and technologies that create leverage of the time and efforts of each cybersecurity professional. Key services and technologies to start investigating offer automation capabilities (for reducing manual processes), leverage artificial intelligence and machine learning (to identify hidden patterns in alert and threat data, among others), orchestration and aggregation (to support better identification and prioritization of threats and incidents), and managed services that will offload much of the labor burden.

Security vendors are investing heavily in AI and ML cybersecurity technologies to improve their offerings.

Sponsor of This White Paper

Anomali® delivers intelligence-driven cybersecurity solutions, these include Anomali ThreatStream®, Anomali Match™, and Anomali Lens™. Private enterprises and public organizations use Anomali to gain unlimited visibility, speed time to detection, and constantly improve security operations. Anomali customers include more than 1,500 global organizations, many of the Global 2000 and Fortune 500, and large government and defense organizations around the world. Founded in 2013, it is backed by leading venture firms including GV, Paladin Capital Group, Institutional Venture Partners, and General Catalyst. Learn more at www.anomali.com

ANOMALI®

www.anomali.com

@Anomali

general@anomali.com

+1 844 484 7328

REFERENCES

[i] NetSec, 47% of UK IT Leaders Say Security Strategies Have Not Been Updated to Account for Their Cloud Environments, August 2020, at https://www.netsec.news/47-of-uk-it-leaders-say-security-strategies-have-not-been-updated-to-account-for-their-cloud-environments/

[ii] ISSA, Cybersecurity Skills Shortage Worsening for Third Year In A Row, Sounding the Alarm for Business Leaders, May 2019, at https://www.globenewswire.com/news-release/2019/05/09/1821287/0/en/Cybersecurity-Skills-Shortage-Worsening-for-Third-Year-In-A-Row-Sounding-the-Alarm-for-Business-Leaders.html

[iii] Kaspersky Lab, Kaspersky Lab Raises Alarm Over Critical Cybersecurity Skills Shortage, Says Youth can Bridge Gap—if Industry Lets it, October 2016, at https://www.prnewswire.com/news-releases/kaspersky-lab-raises-alarm-over-critical-cybersecurity-skills-shortage-says-youth-can-bridge-gap---if-industry-lets-it-598864161.html

[iv] Cybersecurity Skills Shortage Worsening for Third Year In A Row, Sounding the Alarm for Business Leaders, ISSA, May 2019, at https://www.globenewswire.com/news-release/2019/05/09/1821287/0/en/Cybersecurity-Skills-Shortage-Worsening-for-Third-Year-In-A-Row-Sounding-the-Alarm-for-Business-Leaders.html

[v] Cybersecurity Skills Shortage Worsening for Third Year In A Row, Sounding the Alarm for Business Leaders, ISSA, May 2019, at https://www.globenewswire.com/news-release/2019/05/09/1821287/0/en/Cybersecurity-Skills-Shortage-Worsening-for-Third-Year-In-A-Row-Sounding-the-Alarm-for-Business-Leaders.html

[vi] Harvey Nash, Harvey Hash / KPMG CIO Survey 2019—A Changing Perspective, 2019, at https://advisory.kpmg.us/content/dam/advisory/en/pdfs/2019/cio-survey-harvey-nash-2019-full-report.pdf

[vii] ISACA, Survey: Cybersecurity Skills Gap Leaves 1 in 4 Organizations Exposed for Six Months or Longer, February 2017, at https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2017/survey-cyber-security-skills-gap-leaves-1-in-4-organizations-exposed-for-six-months-or-longer

[viii] ISACA, ISACA's State of Cybersecurity 2019 Survey: Retaining Qualified Cybersecurity Professionals Increasingly Challenging for Organizations, March 2019, at https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2019/isacas-state-of-cybersecurity-2019-survey-retaining-qualified-cybersecurity-professionals

[ix] Check Point Research, Cyber Attack Trends: 2020 Mid-Year Report, 2020, at https://www.checkpoint.com/downloads/resources/cyber-attack-trends-report-mid-year-2020.pdf